UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,762	08/06/2003	David S. Abdallah	PRIV-003/01US 307640-2004	1715

22903 7590 08/20/2008

COOLEY GODWARD KRONISH LLP
ATTN: PATENT GROUP
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER	
GERGISO, TECHANE	
ART UNIT	**PAPER NUMBER**
2137	

MAIL DATE	DELIVERY MODE
08/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/635,762	ABDALLAH ET AL.	
	Examiner	Art Unit	
	TECHANE J. GERGISO	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 May 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-21,23-29,32-36 and 38-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-21, 23-29, 32-36 and 38-52* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on May 07, 2008.

2. Claims 15-21, 23-29, 32-36 and 38-52 are pending.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 23 and 28 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 23 recites the following features which are not supported by the specification (see the emphasis):

> "disabling functionality within the personal identification device **except that identification device is configured to send the digital certificate to an enrollment part during future enrollment**"

Claim 28 recites the following features which are not supported by the specification (see the emphasis):

> "the apparatus, the processor configured to receive a digital certificate from the manufacturer party based on the first identifier, **the processor configured to disable functionality of the memory and the processor associated with a party other than an enrollment party**"

However the applicant's disclosure supports the following features which are different form the features recited in claim 23 and 28 above. It only suggests **all functionality within the personal identification device is disabled, such that it is in a state waiting for future enrollment; it does not support as explicitly claim:**

[Applicant's disclosure: 0081] "The personal identification device now generates an asymmetric key pair for itself (step 102). The public key and the device's unique identifier are sent to the manufacturer (step 103). The manufacturer, or other legitimate certificate authority, generates a digital certificate for the device (step 104). This is now sent back to the device, and can be signed by the manufacturer as a token of its legitimacy (step 105). **The manufacturer keeps a record of the device's public key and its unique identifier for future reference (step 106). At this point all functionality within the personal identification device is disabled, such that it is in a state waiting for future enrollment (step 107)**. "

Therefore claim 23 and 28 contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 15-21, 23-29, 32-36 and 38-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Russo et al. (hereinafter referred to as Russo; US Pub. No.: 2003/0115475) in view of Prokoski et al. (Hereinafter referred to as Prokoski, US Pat. No.: 6,850,147).

As per claim 15:

Russo discloses a method, comprising:

receiving at a personal identification device a public key (0006; 0014; 0038);

sending an identifier from the personal identification device to a party based on the public key, the identifier being uniquely associated with the personal identification device (0006; 0048; 0024); and

receiving at the personal identification device a digital certificate from the party based on the identifier, the personal identification device configured to enroll biometric

data after the receiving the public key and after the receiving the digital certificate (0027; 0038; 0048).

Russo does not explicitly teach receiving a public key, sending an identifier and receiving a digital signature before biometric data associated with enrollment is received and disabling functionality within the personal identification device except that identification device is in a wait state with future enrollment. Prokoski, in an analogous art, however teaches receiving a public key, sending an identifier and receiving a digital signature before biometric data associated with enrollment is received and disabling functionality within the personal identification device except that identification device is in a wait state with future enrollment (column 5: lines 30-55; column 6: lines 7-27; column 7: lines 3-23). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Russo to include receiving a public key, sending an identifier and receiving a digital signature before biometric data associated with enrollment is received and disabling functionality within the personal identification device except that identification device is in a wait state with future enrollment. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a system for a personal biometric key that gives reliable results for all persons and to overcome vulnerability of biometric sensors to vandalism, sabotage, degraded performance associated with the need for frequent maintenance, and undetected operational failures as suggested by Prokoski (column 4: lines 65-67; column 5: lines 1-7).

As per claim 16:

Russo discloses a method, further comprising sending the public key from the personal identification device to the party after the receiving the public key (0021; 0025; 0038; 0080).

As per claim 17:

Russo discloses a method, wherein the receiving the digital certificate from the party is based on the public key and the identifier (0021; 0025; 0038; 0080).

As per claim 18:

Russo discloses a method, wherein the identifier is associated with an asymmetric key pair including a personal identification device public key and a personal identification device private key (0038; 0039).

As per claim 19:

Russo discloses a method, further comprising producing the identifier at the personal identification device (0043).

As per claim 20:

Russo discloses a method, further comprising receiving at the personal identification device the identifier from the party (0021; 0025; 0038; 0043; 0080).

As per claim 21:

Russo discloses a method, wherein the digital certificate includes the public key (0021; 0025; 0038; 0043; 0080).

As per claim 23:

Russo discloses a method, comprising:

sending a public key to a personal identification device (0006; 0048; 0024);

receiving an identifier from the personal identification device, the identifier being uniquely associated with the personal identification device (0027; 0038; 0048);

producing a digital certificate based on-the identifier and independent of biometric data (0027; 0038; 0048); and

sending the digital certificate to the personal identification device such that the personal identification device is configured to enroll initial biometric data after the receiving the digital certificate (0006; 0048; 0024).

Russo does not explicitly teach producing digital signature before biometric enrollment and disabling functionality within the personal identification device except that identification device is configured to send the digital certificate to an enrollment part during future enrollment. Prokoski, in an analogous art, however teaches producing digital signature before biometric enrollment and disabling functionality within the personal identification device except that identification device is configured to send the digital certificate to an enrollment part during future enrollment (column 5: lines 30-55; column 6: lines 7-27; column 7: lines 3-23). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the

invention was made to modify the method disclosed by Russo to include producing digital signature before biometric enrollment and disabling functionality within the personal identification device except that identification device is configured to send the digital certificate to an enrollment part during future enrollment. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a system for a personal biometric key that gives reliable results for all persons and to overcome vulnerability of biometric sensors to vandalism, sabotage, degraded performance associated with the need for frequent maintenance, and undetected operational failures as suggested by Prokoski (column 4: lines 65-67; column 5: lines 1-7).

As per claim 24:

Russo discloses a method, wherein the producing of the digital certificate is based, at least in part, on the public key (0021; 0025; 0038; 0080).

As per claim 25:

Russo discloses a method, wherein the receiving and the producing is performed by a first party, the method further comprising (0055):

receiving at the first party a digital certificate uniquely associated with a second party different from the first party (0055-0058);

adding a public key of the first party to the digital certificate associated with the second party (0055-0058); and

sending the digital certificate associated with the second party from the first party to the second party (0055-0058).

As per claim 26:

Russo discloses a method, wherein the digital certificate includes the public key (0021; 0025; 0038; 0080).

As per claim 27:

Russo discloses a method, further comprising producing at the party an asymmetric key pair uniquely associated with the party (0038; 0039).

As per claim 28:

Russo discloses an apparatus, comprising:

a memory configured to store biometric data of a user (0025; 0084);

a processor coupled to the memory and configured to produce a first identifier based on a public key associated with a manufacturer party, the first identifier being uniquely associated with the apparatus (0006; 0024; 0025;0048; 0084);

a biometric sensor coupled to the processor and configured to read biometric input from the user during enrollment (0025; 0040; 0065; 0084); and

a transceiver coupled to the processor and configured to transmit the first identifier to the manufacturer party and a second identifier to a party different from the manufacturer party, the second identifier being uniquely associated with the

biometric input the transceiver being configured to receive the digital certificate (0055-0058).

Russo does not explicitly teach the apparatus, the processor configured to receive a digital certificate from the manufacturer party based on the first identifier the processor configured to disable functionality of the memory and the processor associated with a party other than an enrollment party. Prokoski, in an analogous art, however teaches with the apparatus, the processor configured to receive a digital certificate from the manufacturer party based on the first identifier the processor configured to disable functionality of the memory and the processor associated with a party other than an enrollment party (column 5: lines 30-55; column 6: lines 7-27; column 7: lines 3-23). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Russo to include with the apparatus, the processor configured to receive a digital certificate from the manufacturer party based on the first identifier the processor configured to disable functionality of the memory and the processor associated with a party other than an enrollment party. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a system for a personal biometric key that gives reliable results for all persons and to overcome vulnerability of biometric sensors to vandalism, sabotage, degraded performance associated with the need for frequent maintenance, and undetected operational failures as suggested by Prokoski (column 4: lines 65-67; column 5: lines 1-7).

As per claim 29:

Russo discloses an apparatus, wherein the biometric sensor is a fingerprint sensor configured to read a fingerprint from the user (0040; 0041; 0044).

As per claim 32:

Russo discloses an apparatus, wherein the transceiver includes a radio frequency (RF) (0050)

As per claim 33:

Russo discloses an apparatus, further comprising a visual display coupled to the processor (0006; 0024; 0025; 0048; 0084).

As per claim 34:

Russo discloses a method, comprising:

receiving an encryption identifier at a personal identification device from a party during pr-enrollment (0027; 0038; 0048); and

receiving a digital signature at the personal identification device from the party during the pre-enrolment, the encryption identifier and the digital signature collectively configured to enable verification of the party by the personal identification device (0027; 0038; 0048; 0006; 0048; 0024).

Russo does not explicitly teach disabling functionality within the personal identification device except for functionality associated with future enrollment. Prokoski, in an analogous art, however teaches disabling functionality within the personal identification device except for functionality associated with future enrollment (column 5: lines 30-55; column 6: lines 7-27; column 7: lines 3-23). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Russo to include disabling functionality within the personal identification device except for functionality associated with future enrollment. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire to provide a system for a personal biometric key that gives reliable results for all persons and to overcome vulnerability of biometric sensors to vandalism, sabotage, degraded performance associated with the need for frequent maintenance, and undetected operational failures as suggested by Prokoski (column 4: lines 65-67; column 5: lines 1-7).

As per claim 35:

Russo discloses a method, wherein: the encryption identifier is a public key (0027; 0038); and the receiving the digital signature including receiving a digital certificate including the digital signature (0027; 0038; 0048).

As per claim 36:

Russo discloses a method, wherein: the encryption identifier is a public key (0027; 0038); and the receiving the digital signature including receiving a digital certificate including the digital signature based on the public key (0027; 0038; 0048).

As per claim 38:

Russo disclose the party is a manufacturer of the personal identification device and separate from an enrollment party authorized to enable enrollment of the biometric data at the personal identification device (0050).

As per claims 39:

Russo disclose the party is a first party, the personal identification device being configured to enroll the biometric data from a second party different from the first party after the receiving at the personal identification device the digital certificate (0070).

As per claim 40:

Russo disclose the digital certificate includes data associated with the personal identification device (0071-0073).

As per claim 41:

Russo disclose the party is a manufacturer of the personal identification device and separate from the enrollment party authorized to enable enrollment of the biometric data at the personal identification device (0050).

As per claim 42:

Russo disclose the personal identification device is configured to enroll biometric data from the enrollment party after the sending the digital certificate (0006; 0048; 0024).

As per claim 43:

Russo disclose the producing the digital certificate is based on data associated with the personal identification device (0071-0073).

As per claim 44:

Russo disclose the transceiver is configured to receive the digital certificate from the manufacturer party.

As per claim 45:

Russo disclose the party is an enrollment authority of the biometric data (0027; 0038; 0048).

As per claim 46:

Russo disclose the digital certificate includes data associated with the apparatus (0071-0073).

As per claim 47:

Russo disclose the party is a manufacturer of the personal identification device (0027; 0038; 0048).

As per claim 48:

Russo disclose the party is a first party, the personal identification device being configured to enroll biometric data from a second party different from the first party after the receiving the encryption identifier and after receiving the digital certificate (0006; 0048; 0024).

As per claim 49:

Russo disclose the digital signature includes data associated with the personal identification device (0071-0073).

As per claim 50:

Prokoski disclose the method, wherein the wait state associated with future enrollment is a first wait state associated with future enrollment (column 5: lines 30-55; column 6: lines 7-27; column 7: lines 3-23).

As per claim 51:

Prokoski disclose the method, wherein the future enrollment is a first future enrollment (column 5: lines 30-55; column 6: lines 7-27; column 7: lines 3-23).

As per claim 2

Prokoski disclose the method, wherein the future enrollment is a first future enrollment (column 5: lines 30-55; column 6: lines 7-27; column 7: lines 3-23).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Techane J. Gergiso** whose telephone number is **(571) 272-3784** and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Emmanuel Moise** can be reached on **(571) 272-3865**. The fax phone number for the organization where this application or proceeding is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137